⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭61－177479

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和61年(1986)8月9日
G 09 C 1/00		7368－5B	
G 06 F 12/00		6974－5B	

審査請求　未請求　発明の数 1　（全9頁）

⑤4発明の名称　暗号化鍵管理方式

⑳特　願　昭60－16618
㉒出　願　昭60(1985)2月1日

⑦2発明者　中井　敏久　東京都港区虎ノ門1丁目7番12号　沖電気工業株式会社内
⑦1出願人　沖電気工業株式会社　東京都港区虎ノ門1丁目7番12号
⑦4代理人　弁理士　鈴木　敏明

明　細　書

1. 発明の名称

暗号化鍵管理方式

2. 特許請求の範囲

電子ファイルの機密保護に階層構造を持った暗号化鍵を用いるシステムの暗号化鍵管理方式において、

(a) 暗号化鍵が階層順にマスタ鍵、ファイル鍵、ワーク鍵から成り、

(b) 消失誤り訂正符号化されたファイル鍵を利用者の数だけ発生させ、各利用者に分配する手段と、

(c) 各利用者が独自に設定したマスタ鍵で各自のファイル鍵を暗号化する手段と、

(d) 前記(c)項の手段で暗号化されたファイル鍵を蓄積する手段と、

(e) 前記(d)項の手段に蓄積されている暗号化されたファイル鍵を読出し、各利用者のマスタ鍵で復号化する手段と、

(f) データファイルを暗号化するワーク鍵をデータファイルの数だけ発生する手段と、

(g) データファイルを前記ワーク鍵で暗号化する手段と、

(h) 前記ワーク鍵を各利用者のファイル鍵で暗号化する手段と、

(i) 前記(g)項の手段で暗号化されたデータファイルと前記(h)項で暗号化されたワーク鍵とを結合して蓄積する手段と、

(j) 前記(i)項の手段から暗号化されたワーク鍵を読み出し、各利用者のファイル鍵で復号化する手段と、

(k) 前記(j)項の手段で復号化されたワーク鍵を用いて、該ワーク鍵が暗号化されていた時に結合していた暗号化されたデータファイルを復号化する手段と、

(l) マスタ鍵のうちの1つを紛失した時には、他の利用者のファイル鍵から前記マスタ鍵によって暗号化される前のファイル鍵を前記(b)項の消失誤り訂正のアルゴリズムによって復元する手段と、

を備えてなる暗号化鍵管理方式。

3. 発明の詳細な説明

（産業上の利用分野）

本発明は、電子ファイルの機密保護に暗号化を用いた場合の暗号化鍵管理方式に関する。

（従来の技術）

従来、特開昭54-87032公報、並びに「データ保護と暗号化の研究」（P90～97、日本経済新聞社）に記載されているように、電子ファイルの機密保護のための暗号化鍵管理方式としては、3階層の鍵管理方式がある。この方式では暗号化鍵として、データ暗号化鍵であるワーク鍵（WK）と、ワーク鍵を暗号化するファイル鍵（FK）と、ファイル鍵を暗号化するマスタ鍵（MK）の3種を設けている。上記暗号化鍵のうち、ワーク鍵はデータファイル毎に異なったものが割り当てられ、ファイル鍵は管理プログラムにより利用者毎に割り当てられる。また、マスタ鍵は前記管理プログラムにより自動作成されるか、あるいはシステム管理者により入力され、前記管理プログラムにより保護された部分に蓄積される様になっており、ホスト計算機に唯1個存在する。

第7図は暗号化鍵の階層構造の一例を示す説明図である。同図中、MKはマスタ鍵、FK_i（i＝1，2，3）は利用者iに割り当てられたファイル鍵、WK_j（j＝1，2，…7）はデータファイルjに割り当てられたワーク鍵である。同図は下位の鍵が上位の鍵によって暗号化され、格納されることを示しており、以下第8図、第9図を用いて、その暗号化の動作を説明する。

第8図はファイル鍵の暗号化を示す説明図、第9図はデータファイルの暗号化を示す説明図である。まず、管理プログラムは第8図に示すように、ファイル鍵発生部81において任意にファイル鍵FK_iを発生させ、マスタ鍵MKを用いて暗号化部83で暗号化し、ファイル鍵メモリ82に蓄積する。尚、以下$E_{x(y)}$は暗号化鍵xでyを暗号化したものを表すものとする。

次に、第9図に示すように、利用者iがデータファイル91を暗号化しようとする場合、管理プログラムはパスワード等により利用者iが確かに利用者i本人であることを確認した後、ファイル鍵メモリ82から$E_{MK}(FK_i)$を取り出し、マスタ鍵MKを用いて復号化部93で復号化し、ファイル鍵FK_iを利用者iに与える。利用者iはワーク鍵発生部90より発生したワーク鍵WKを前記FK_iを用いて暗号化部94で暗号化し、その結果として$E_{FKi}(WK)$を暗号化データファイル92のヘッダ部分に書き込む。そして、利用者iはワーク鍵WKを用いてデータファイル91のデータdataを暗号化部95で暗号化し、暗号化データファイル92に$E_{WK}(data)$として蓄積する。

このようにすると、利用者iが暗号化データファイル92を復号化しようとする場合には、まずパスワード等によって本人確認をすると、管理プログラムがファイル鍵メモリ82から$E_{MK}(FK_i)$を読み出し、マスタ鍵MKを用いて復号化し、ファイル鍵FK_iを利用者iに与える。そして利用者iは暗号化データファイル92のヘッダ部分に書き込まれている$E_{FKi}(WK)$を読み出して、ファイル鍵FK_iで復号化してワーク鍵WKを得、さらに前記WKで暗号化データファイル92に蓄積されている$E_{WK}(data)$を復号化して、所望のデータを得ることになる。

なお、前述した暗号化部、及び復号化部は各々独立した暗号化←→復号化のアルゴリズムを用いたリフトウェアモジュールでも良いし、同一の暗号化←→復号化のアルゴリズムを用いたリフトウェアモジュールを時分割的に共有してもかまわない。

この方式によれば、暗号化データファイルの数が増大し、ワーク鍵の数が増えても、マスタ鍵ただ1つを不正な利用者からアクセスされないように管理プログラムが秘密に保護すればファイルの機密を保つことができる。また何らかの理由でマスタ鍵を変更する時も、ファイル鍵メモリ82の内容だけを書きかえればよく、膨大な暗号化データファイルを書きかえる必要がないという利点があった。

（発明の解決しようとする問題点）

しかしながら、上述した方式では機密の責任が

ただ1つのマスタ鍵に集中するため、管理プログラムが各利用者の確認をしなければならない事、メモリ中に秘密の領域を設けなければならない事、及び1つしかないマスタ鍵を何らかの理由で紛失すると全ての暗号化ファイルの復号化が不可能になる事、等の問題点があった。

（問題点を解決するための手段）

本発明は上述の問題点に鑑み、電子ファイルの機密保護にマスタ鍵、ファイル鍵、ワーク鍵から成る階層構造を持った暗号化鍵を用いるシステムの暗号化鍵管理方式において、消失誤り訂正符号化されたファイル鍵を利用者の数だけ発生させ、各利用者に分配するファイル鍵分配部11と、各利用者が独自に設定したマスタ鍵で各自のファイル鍵を暗号化する暗号化部12と、前記暗号化部12で暗号化されたファイル鍵を蓄積するファイル鍵メモリ13と、前記ファイル鍵メモリ13に蓄積されている暗号化されたファイル鍵を読出し、各利用者のマスタ鍵で復号化する復号化部14、及び31と、データファイルを暗号化するワーク鍵をデータファイルの数だけ発生するワーク鍵発生部90と、データファイルを前記ワーク鍵で暗号化する暗号化部15と、前記ワーク鍵を各利用者のファイル鍵で暗号化する暗号化部15と、前記暗号化部16によって暗号化されたデータファイルのヘッダ部分に前記暗号化部15で暗号化されたワーク鍵を書きこんで蓄積する暗号化データファイル92と、前記暗号化データファイル92から暗号化されたワーク鍵を読み出し、各利用者のファイル鍵で復号化する復号化部32と、前記復号化部32によって復号化されたワーク鍵を用いて、該ワーク鍵が暗号化されてヘッダ部分に書きこまれていた暗号化データファイルを読み出して復号化する復号化部33と、マスタ鍵のうちの1つを紛失した時には他の利用者のファイル鍵から前記マスタ鍵によって暗号化される前のファイル鍵を消失誤り訂正のアルゴリズムによって復元する手段、とを備えてなる暗号化鍵管理方式であり、以下その作用、動作を実施例を用いて詳細に説明する。

（実施例）

第1図は本発明の実施例の、暗号化の動作を説明するためのブロック図である。管理プログラムはファイル鍵分配部11において各利用者にファイル鍵を発生し、利用者i（i＝1，2，…N）にファイル鍵FK_iを配布する。利用者iは自らが設定し記憶するマスタ鍵MK_iを用いて暗号化部12においてFK_iを暗号化し$E_{MKi}(FK_i)$を作成してファイル鍵メモリ13に蓄積する。

次にデータファイル91の暗号化について説明する。まず利用者iはマスタ鍵MK_iを入力し、ファイル鍵メモリ13に蓄積されている$E_{MKi}(FK_i)$をMK_iを用いて復号化部14で復号し利用者iのファイル鍵FK_iをえる。つづいて、ワーク鍵発生部90において任意にワーク鍵WKを発生し、ファイル鍵FK_iを用いてワーク鍵WKを暗号化部15において暗号化し、$E_{FKi}(WK)$を暗号化データファイル92のヘッダ部分に記録する。さらにデータファイル91を、ワーク鍵WKを用いて暗号化部16で暗号化し$E_{WK}(data)$を得て、暗号化データファイル92に蓄積する。

この様にした場合の暗号化鍵の管理方式を第2図を用いて説明する。第2図は本実施例において、利用者数＝N＝3の場合の暗号化鍵の階層管理の一例を示した図である。同図中、下位の鍵は上位の鍵で暗号化した形で保存され、最上位の鍵であるマスタ鍵MK_iは各利用者iにより秘密に保管される。利用者1と利用者2のマスタ鍵が異なるので、たとえ利用者1が$E_{MK2}(FK_2)$を手に入れても利用者2のマスタ鍵MK_2を知らない限り、FK_2を得ることができない。したがって利用者2以外が利用者2の暗号化データファイルを復号することはできない。また利用者1が自分のマスタ鍵を変更したい時は、第1図のファイル鍵メモリ13の$E_{MKi}(FK_i)$のみを変更すればよく、暗号化データファイル92を変更する必要はない。

さらに、本実施例における復号化の動作を第3図を用いて説明する。第3図は本実施例の復号化の動作を説明するためのブロック図である。利用者iが暗号化データファイル92を復号化する場

合、まず利用者iは自分のマスタ鍵MK_iを入力し、ファイル鍵メモリ13に蓄積されている$E_{MKi}(FK_i)$を復号化部31で復号化し、自らのファイル鍵FK_iを得る。次に暗号化データファイル92のヘッダ部分に記録されている$E_{FKi}(WK)$を前記FK_iを用いて復号化部32で復号化し、ワーク鍵WKを得る。そして最後に暗号化データファイル92に蓄積されている$E_{WK}(data)$を前記ワーク鍵WKを用いて復号化部33で復号化し、データファイル91に格納するのである。

次に、第1図におけるファイル鍵分配部11の機能について説明し、本実施例のあるマスタ鍵が紛失した時の動作を説明する。

第4図は第1図におけるファイル鍵分配部11の内部を示すブロック図である。いまホスト計算機システムの利用者の数をNとする。まずホスト計算機の管理プログラムは、N－1個のファイル鍵発生部41で、任意にN－1個のファイル鍵$FK_1, FK_2, \cdots FK_{N-1}$を発生する。次に消失誤り訂正符号化部42で前記$FK_1, FK_2, \cdots FK_{N-1}$を情報点とし、検査点$FK_N$を生成する。そして、$FK_1, FK_2, \cdots FK_{N-1}, FK_N$を各利用者のファイル鍵として分配する。

第5図は、ある利用者k（$1 \leq k \leq N$）がマスタ鍵を紛失した場合に、該利用者kのファイル鍵を復元する動作を説明するためのブロック図である。

まず利用者k以外の利用者は各自のマスタ鍵で各自のファイル鍵を復号する。例えば利用者1はファイル鍵メモリ51の$E_{MK1}(FK_1)$をMK_1を用いて復号化部52で復号し、FK_1を得る。この動作によりN個のファイル鍵のうちFK_kを除くN－1個が消失誤り訂正復号化部56に入力される。消失誤り訂正復号化部56では通常の消失誤り訂正の手法により利用者iのファイル鍵FK_kを復元する。利用者kは新しく任意にマスタ鍵MK_k'を設定し暗号化部57により暗号化してその結果の$E_{MKk}'(FK_k)$をファイル鍵メモリ58に格納する。以降の暗号データファイルの復号化および、データファイルの暗号化は、新しいマスタ鍵MK_kによって行なえばよいことになる。

消失誤り訂正符号としては、ファイル鍵の長さ以上の長さの消失バースト誤りを訂正できる符号であれば、どのような符号も本発明に適用可能である。

消失バースト誤り訂正符号化と復号化を簡単に第6図を用いて説明する。ここでは符号としては情報点数が2、検査点数が1の1消失誤り訂正符号をファイル鍵長だけインタリーブして、ファイル鍵長の消失バースト誤りを訂正できる符号を用い、利用者数はN＝3とする。まず利用者1のファイル鍵FK_1と利用者2のファイル鍵FK_2を任意に発生する。次にFK_1とFK_2の各ビットの排他的論理和をとったものをFK_3とする。すると、

$$FK_1 = FK_2 \oplus FK_3 \quad \cdots\cdots (1)$$

$$FK_2 = FK_1 \oplus FK_3 \quad \cdots\cdots (2)$$

$$FK_3 = FK_1 \oplus FK_2 \quad \cdots\cdots (3)$$

の関係が成立する。したがってFK_1, FK_2, FK_3の3つのうちの1つを紛失しても他の2つが揃えば紛失したファイル鍵を復元できる。たとえばFK_1を紛失すれば式(1)を用いればよいのである。

（発明の効果）

以上、実施例を用いて説明したように、本発明によれば以下に示すような効果が得られる。

① 管理プログラムによる利用者の確認や、管理プログラムにより保護された秘密の領域が不要となり、暗号化データファイルの安全性が向上する。

② 利用者は自分自身の1つのマスタ鍵のみを秘密に保てば、多くのファイルの機密を保持することができる。

③ 利用者は自分自身のマスタ鍵を容易に変更することができるため安全性が向上する。

④ ある利用者がマスタ鍵を紛失しても、暗号化データファイルが復号不可能になることはないため、暗号化システムの信頼性が向上する。

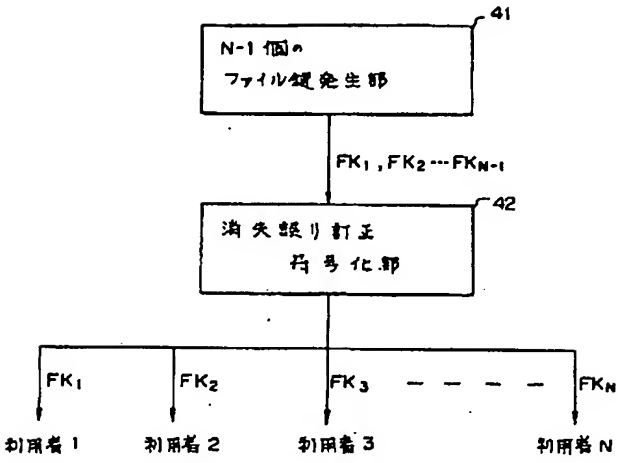
4. 図面の簡単な説明

第1図は本発明の実施例の暗号化の動作を説明するブロック図、第2図は本発明の実施例において、利用者数＝3の場合の暗号化鍵の階層管理の

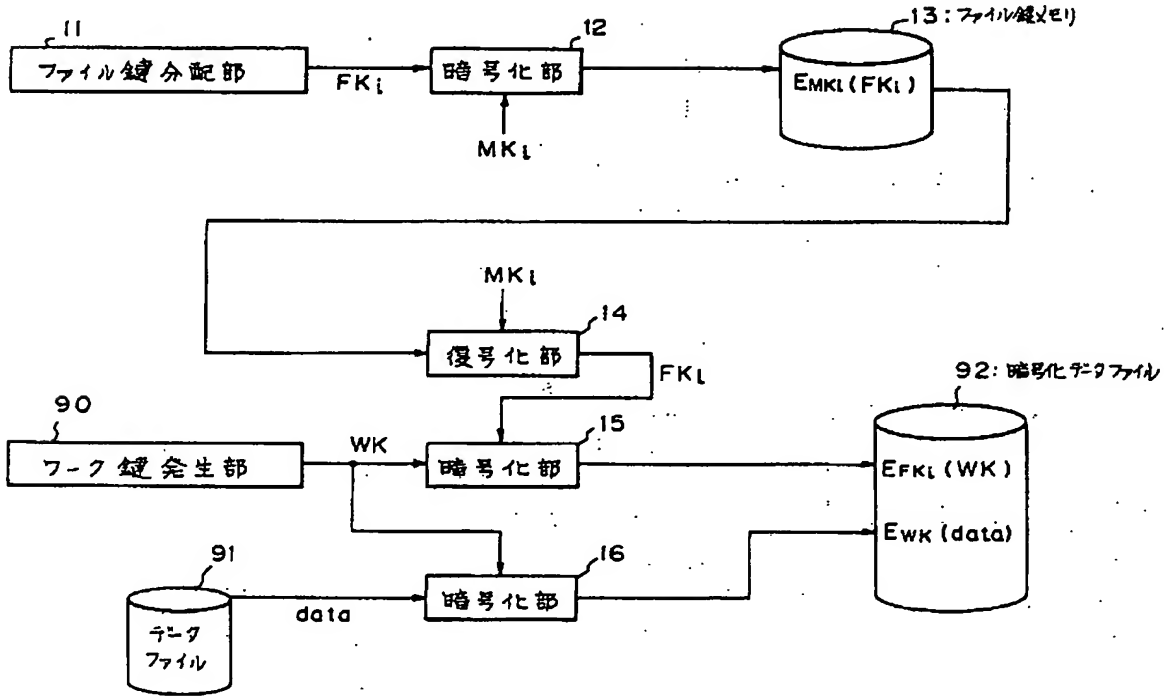
一例を示す図、第3図は本発明の実施例の復号化の動作を説明するブロック図、第4図は第1図におけるファイル鍵分配部11の内部を示すブロック図、第5図は、本発明の実施例において、ある利用者kが自分のマスタ鍵を紛失した場合に、該利用者kのファイル鍵を復元する動作を説明するブロック図、第6図はファイル鍵の消失バースト訂正誤りを説明する図、第7図は従来の暗号化鍵の階層構造の一例を示す図、第8図は従来のファイル鍵の暗号化の動作を説明する説明図、第9図は従来のデータファイルの暗号化の動作を説明する説明図である。

11…ファイル鍵分配部、12，15，16，57…暗号化部、13，51，58…ファイル鍵メモリ、14，31，32，33，52，53，54，55…復号化部、90…ワーク鍵発生部、91…データファイル、92…暗号化データファイル、41…N－1個のファイル鍵発生部、42…消失誤り訂正符号化部、56…消失誤り訂正復号化部。

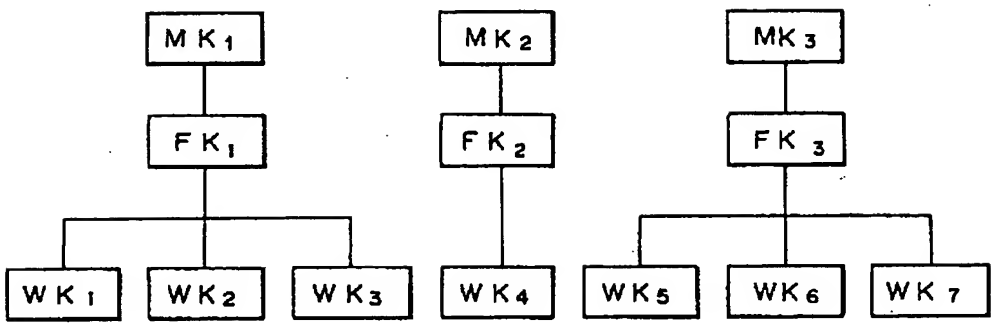
第4図



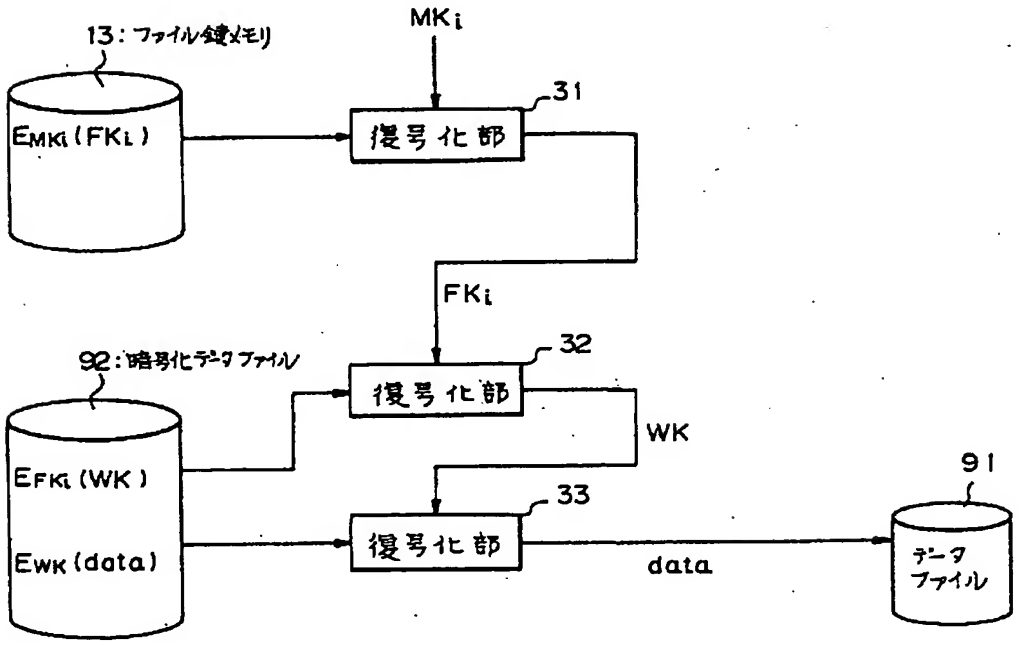
第1図



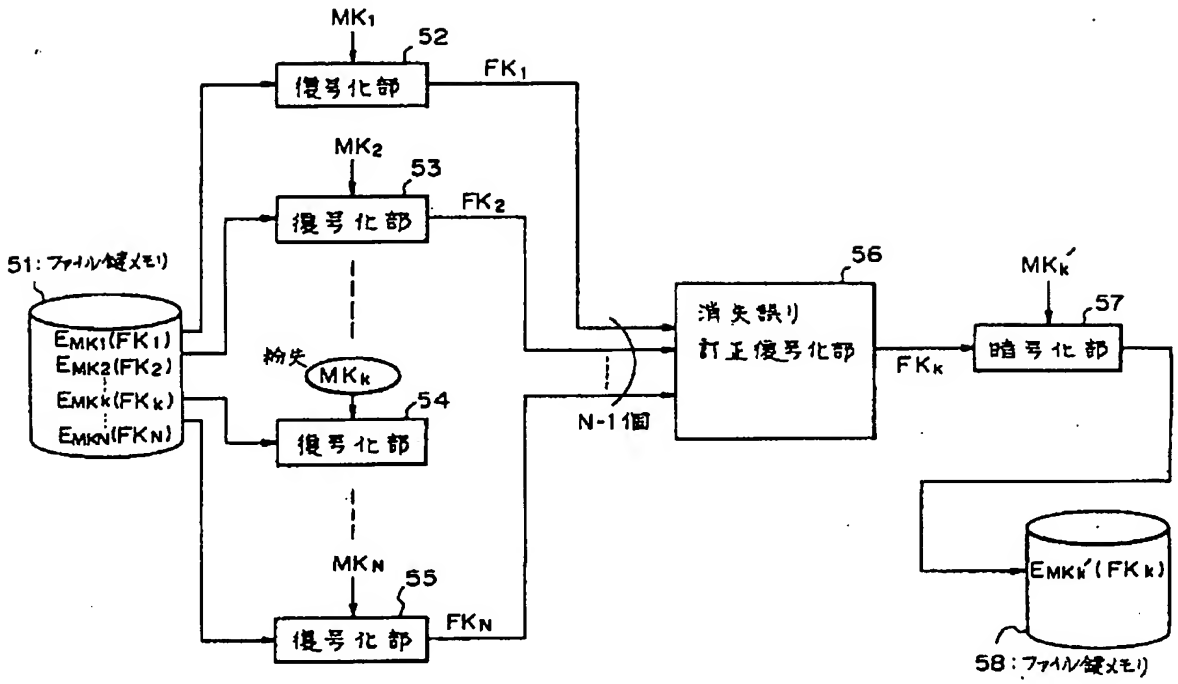
第２図


MK1
MK2
MK3
FK1
FK2
FK3
WK1
WK2
WK3
WK4
WK5
WK6
WK7

第３図


13：ファイル鍵メモリ
MKi
31
EMKi(FKi)
復号化部
FKi
92：暗号化データファイル
32
復号化部
WK
EFKi(WK)
EWK(data)
33
復号化部
91
data
データファイル

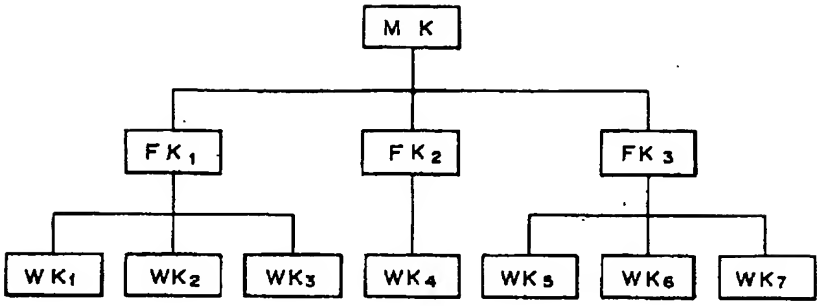
第５図



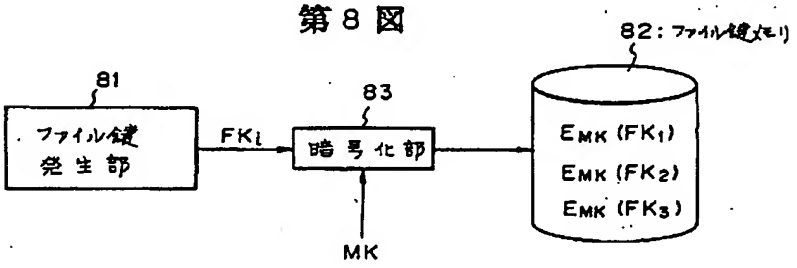
第６図

FK_1	1	1	0	1	1	—	—	—	1	0	0	1	0	0
FK_2	0	1	0	1	1	—	—	—	0	1	1	1	1	1
FK_3	1	0	0	0	0	—	—	—	1	1	1	0	1	1

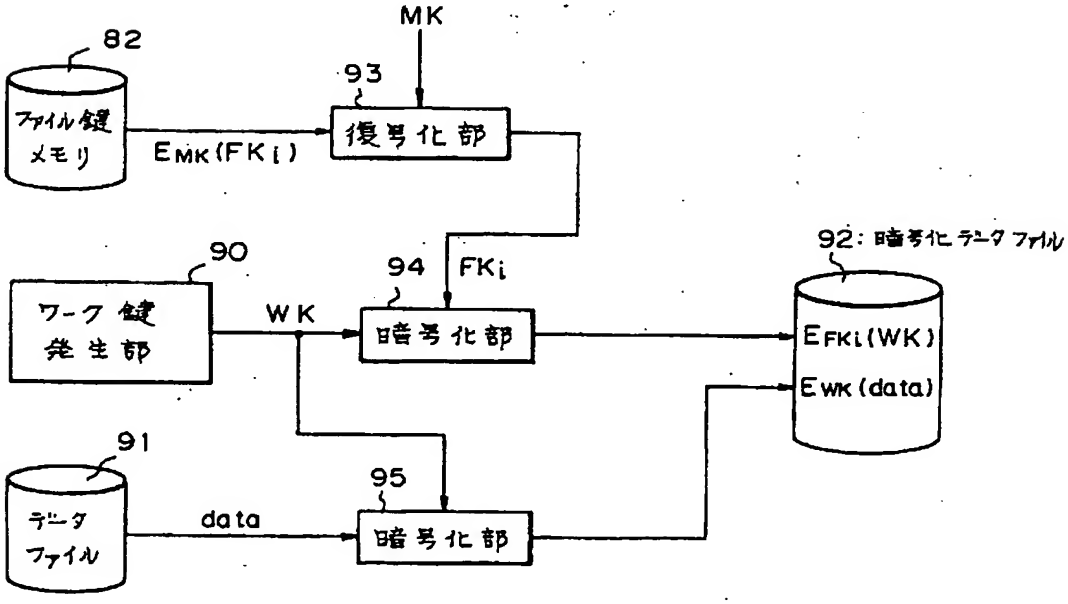
第7図


MK
FK1
FK2
FK3
WK1
WK2
WK3
WK4
WK5
WK6
WK7

第8図


82：ファイル鍵メモリ
81
ファイル鍵
発生部
FKi
83
暗号化部
MK
EMK(FK1)
EMK(FK2)
EMK(FK3)

第9図


MK
82
93
ファイル鍵
メモリ
EMK(FKi)
復号化部
92：暗号化データファイル
90
94
FKi
ワーク鍵
発生部
WK
暗号化部
EFKi(WK)
EWK(data)
91
95
データ
ファイル
data
暗号化部

手続補正書（自発）

昭和 60.6.24 年 月 日

特許庁長官 殿

1. 事件の表示

昭和60年 特 許 願第 016618 号

2. 発明の名称

暗号化鍵管理方式

3. 補正をする者

事件との関係 特許出願人

住 所(〒105) 東京都港区虎ノ門1丁目7番12号

名 称(029) 沖電気工業株式会社

代表者 取締役社長 橋本南海男

4. 代 理 人

住 所(〒105) 東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社内

氏 名(6892) 弁理士 鈴木敏明

電話 501-3111(大代表)

補正の対象 明細書中「特許請求の範囲」の欄及び「発明の詳細な説明」の欄

補正の内容 別紙の通り

6. 補正の内容

(1) 明細書中「特許請求の範囲」の欄を別紙のとおり補正する。

(2) 同書第4頁第16行目に、「以下Ex(y)は暗号化鍵xでyを暗号化した」とあるのを「以下Ex(Y)は暗号化鍵xでYを暗号化した」と補正する。

(3) 同書第6頁第6行目、第7行目及び第8行目に「リフトウェアモジュール」とあるのを「ソフトウェアモジュール」と補正する。

(4) 同書同頁第13行目に、「プログラムが秘密に」とあるのを「プログラムがパスワード等により秘密に」と補正する。

以 上

特許請求の範囲

電子ファイルの機密保護に階層構造を持った暗号化鍵を用いるシステムの暗号化鍵管理方式において、

(a) 暗号化鍵が階層順にマスタ鍵、ファイル鍵、ワーク鍵から成り、

(b) 消失誤り訂正符号化されたファイル鍵を利用者の数だけ発生させ、各利用者に分配する手段と、

(c) 各利用者が独自に設定したマスタ鍵で各自のファイル鍵を暗号化する手段と、

(d) 前記(c)項の手段で暗号化されたファイル鍵を蓄積する手段と、

(e) 前記(d)項の手段に蓄積されている暗号化されたファイル鍵を読出し、各利用者のマスタ鍵で復号化する手段と、

(f) データファイルを暗号化するワーク鍵をデータファイル毎に発生する手段と、

(g) データファイルを前記ワーク鍵で暗号化する手段と、

(h) 前記ワーク鍵を各利用者のファイル鍵で暗号化する手段と、

(i) 前記(g)項の手段で暗号化されたデータファイルと前記(h)項で暗号化されたワーク鍵とを蓄積する手段と、

(j) 前記(i)項の手段から暗号化されたワーク鍵を読み出し、各利用者のファイル鍵で復号化する手段と、

(k) 前記(j)項の手段で復号化されたワーク鍵を用いて、該ワーク鍵によって暗号化されたデータファイルを復号化する手段と、

(l) マスタ鍵のうちの1つを紛失した時には、他の利用者のファイル鍵から前記マスタ鍵によって暗号化される前のファイル鍵を前記(b)項の消失誤り訂正のアルゴリズムによって復元する手段と、

を備えてなる暗号化鍵管理方式。